Amendments to the Claims

This listing of claims will replace all prior versions and listings of claims in the subject application.

Listing of Claims:

What is claimed is:

1. (Previously Presented): An integrated firewall/VPN system, comprising:

at least one wide area network (WAN);

at least one local area network (LAN); and

an integrated firewall/VPN chipset configured to send and receive data packets between said WAN and said LAN, said chipset comprising:

a firewall comprising a first layer including a header match packet filtering engine configured to provide pattern matching in selected headers of data, a second layer including a contents match packet filtering engine configured to analyze the scope of at least one data packet, a third layer including at least one application proxy configured to provide additional pattern matching using a hardware engine configured to provide pre-analysis processing to reduce the workload of a central processing unit (CPU) and a fourth layer including a session match engine configured to store a TCP/UDP connection setup in a look-up-table and to forward the setup progress to said CPU for tracking;

a VPN configured to provide security functions for data between said LAN and said WAN, wherein said security functions are selected from the group consisting of encryption, decryption, encapsulation, and decapsulation of said data packets, said VPN including a VPN packet buffer configured to receive at least one of said data packets and to forward said at least one data packet to an inbound VPN processor configured to decrypt and decapsulate said at least one data packet, said VPN further including an inbound security database having a database of tunnels configured to provide said inbound VPN processor with tunnel information used to decrypt and decapsulate said at least one data packet, said VPN further including protocol instructions having microcodes configured to instruct said VPN processor to decrypt and decapsulate said at least one data packet according to a user-defined security procedure; and

an interface configured to determine if said data packets are plain text or cipher text, said interface further configured to forward a preselected number of bytes to said firewall if said data packets are plain text, said interface further configured to forward said data packets to said VPN if said data packets are cipher text.

2. (Previously Presented): A system as claimed in claim 1, wherein said chipset further comprises a router adapted to route data between said WAN and said LAN.

3. (Previously Presented): A system as claimed in claim 1, wherein said firewall is configured to provide static and/or dynamic data packet filtering.

4. (Previously Presented): A system as claimed in claim 3, wherein said header match packet filtering engine is configured to provide pattern matching in selected headers of said data and their combination from L2, L3 and L4 headers.

5. (Previously Presented): A system as claimed in claim 1, wherein said chipset is further configured to analyze access control functions based on preselected bytes of said data packets.

6. (Original): A system as claimed in claim 5, wherein said preselected bytes comprise the first 144 bytes of said data packet.

7. (Cancelled):

8. (Previously Presented): A system as claimed in claim 1, wherein said firewall further includes access control functions comprising user-defined access control protocols.

9. (Previously Presented): A firewall/VPN integrated circuit (IC), comprising:

a router core configured to interface between at least one untrusted network and at least one trusted network to send and receive data packets between said untrusted and said trusted

networks;

a firewall system, comprising a first layer including a header match packet filtering engine configured to provide pattern matching in selected headers of data, a second layer including a contents match packet filtering engine configured to analyze the scope of at least one data packet, a third layer including at least one application proxy configured to provide additional pattern matching using a hardware engine configured to provide pre-analysis processing to reduce the workload of a central processing unit (CPU) and a fourth layer including a session match engine configured to store a TCP/UDP connection setup in a look-up-table and to forward the setup progress to said CPU for tracking;

a VPN configured to provide security functions for data between said at least one untrusted and said at least one trusted network, wherein said security functions comprise encryption, decryption, encapsulation, and decapsulation of said data packets, said VPN including a VPN packet buffer configured to receive at least one of said data packets and to forward said at least one data packet to an inbound VPN processor configured to decrypt and decapsulate said at least one data packet, said VPN further including an inbound security database having a database of tunnels configured to provide said inbound VPN processor with tunnel information used to decrypt and decapsulate said at least one data packet, said VPN further including protocol instructions having microcodes configured to instruct said VPN processor to decrypt and decapsulate said at least one data packet according to a user-defined security procedure; and

an interface configured to determine if said data packets are plain text or cipher text, said interface further configured to forward a preselected number of bytes to said firewall if said data packets are plain text, said interface further configured to forward said data packets to said VPN if said data packets are cipher text.

10. (Previously Presented): An IC as claimed in claim 9, wherein said firewall system is configured to provide static and/or dynamic data packet filtering.

11. (Previously Presented): An IC as claimed in claim 10, header match packet filtering circuit

is configured to provide pattern matching in selected headers of said data and their combination from L2, L3 and L4 headers.

12. (Previously Presented): An IC as claimed in claim 9, wherein said firewall system is further configured to analyze access control functions based on preselected bytes of said data packets.

13. (Original): An IC as claimed in claim 12, wherein said preselected bytes comprise the first 144 bytes of said data packet.

14. (Cancelled):

15. (Previously Presented): An IC as claimed in claim 9, wherein said firewall system further includes access control functions comprising user-defined access control protocols.

16. (Previously Presented): A method of providing firewall access control functions, comprising the steps of:

defining one or more access control protocols;

receiving a data packet at an interface configured to determine if said data packet is plain text or cipher text, said interface further configured to forward a preselected number of bytes to a firewall system if said data packets includes plain text, said interface further configured to forward said data packets to a VPN if said data packet includes cipher text;

selecting a certain number of bytes of said data packet if said data packet includes plain text;

processing said selected bytes using said access control protocols via said firewall system, said firewall system comprising a first layer including a header match packet filtering engine configured to provide pattern matching in selected headers of data, a second layer including a contents match packet filtering engine configured to analyze the scope of said data packet, a third layer including at least one application proxy configured to provide additional

pattern matching using a hardware engine configured to provide pre-analysis processing to reduce the workload of a central processing unit (CPU) and a fourth layer including a session match engine configured to store a TCP/UDP connection setup in a look-up-table and to forward the setup progress to said CPU for tracking; and

receiving at least one cipher text data packet at a VPN configured to provide security functions for data between said LAN and said WAN, wherein said security functions are selected from the group consisting of encryption, decryption, encapsulation, and decapsulation of said at least one cipher text data packet, said VPN including a VPN packet buffer configured to receive said at least one cipher text data packet and to forward said at least one cipher text data packet to an inbound VPN processor configured to decrypt and decapsulate said at least one cipher text data packet, said VPN further including an inbound security database having a database of tunnels configured to provide said inbound VPN processor with tunnel information used to decrypt and decapsulate said at least one cipher text data packet, said VPN further including protocol instructions having microcodes configured to instruct said VPN processor to decrypt and decapsulate said at least one cipher text data packet according to a user-defined security procedure.

17. (Cancelled)